(19)日本国特許庁（ＪＰ） (12) 公開特許公報（A） (11)特許出願公開番号

特開平5－53921

(43)公開日 平成5年(1993)3月5日

(51)Int.Cl.[5]		識別記号	庁内整理番号	FI	技術表示箇所
G06F	12/14	320 B	9293－5B		
	15/78	510 Z	7530－5L		
G09C	1/00		7922－5L		

審査請求 未請求 請求項の数3(全 7 頁)

(21)出願番号 特願平3－237147

(22)出願日 平成3年(1991)8月23日

(71)出願人 000006655
新日本製鐵株式会社
東京都千代田区大手町２丁目６番３号

(72)発明者 佐々木 圓
東京都千代田区大手町２－６－３ 新日本製鐵株式会社内

(72)発明者 柴田 尚宰
東京都千代田区大手町２－６－３ 新日本製鐵株式会社内

(72)発明者 成田 喜則
東京都千代田区大手町２－６－３ 新日本製鐵株式会社内

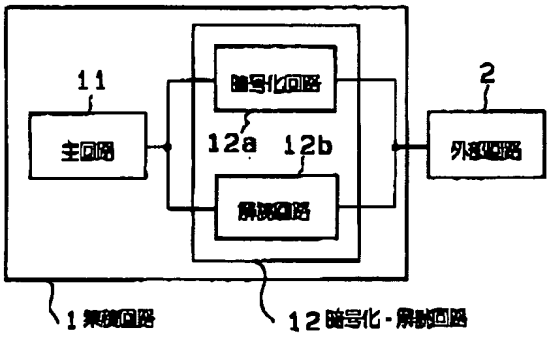
(74)代理人 弁理士 國分 孝悦

(54)【発明の名称】 集積回路

(57)【要約】

【目的】 外部回路と接続されてデータの入出力を行う集積回路において、データの複製および回路の機能の複製を防止する。

【構成】 集積回路１に、主たる機能を実現する主回路１１、暗号化解読回路１２を設けた。暗号化解読回路１２は、主回路１１から出力されたデータを暗号化し外部回路２へ出力する暗号化回路１２ａと外部回路２から入力された暗号化されたデータを解読し主回路１１へ出力する解読回路１２ｂを有している。集積回路１に入出力されるデータを複製しても主回路１１の機能のみを複製した回路では使用できない。また、データが暗号化されているため、主回路の複製も困難である。



1

【特許請求の範囲】

【請求項1】 外部装置との間でデータの入出力が行われ、該入出力されるデータを処理する集積回路において、該集積回路は、

前記集積回路の機能に基づく種々の動作を行う主回路手段と、

前記入出力されるデータを暗号化または解読する暗号処理手段とを有し、

前記外部装置との間で暗号化されたデータの入出力が行われることを特徴とする集積回路。

【請求項2】 外部装置との間でデータの入出力が行われ、該入出力されるデータを処理する集積回路において、該集積回路は、

前記集積回路の機能に基づく種々の動作を行う主回路手段と、

前記主回路手段から出力されるデータを暗号化する暗号化手段と、前記外部装置から入力される暗号化されたデータを解読する解読手段とからなる暗号処理手段とを有し、

前記外部装置との間で暗号化されたデータの入出力が行われることを特徴とする集積回路。

【請求項3】 前記主回路手段がＣＰＵであり、前記集積回路は１チップに形成された１チップマイクロコンピュータであることを特徴とする請求項２に記載の集積回路。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、外部装置に接続されてデータの入出力を行う集積回路に関し、授受されるデータの複製および集積回路の機能の複製を防止できる集積回路に関する。

【０００２】

【従来の技術】従来、接続される回路すなわち外部装置とデータの入出力を行う集積回路は、入出力されるデータの複製を防止するために、システムを構成する集積回路以外のハードウエアを利用した複製防止データをデータの一部として組み込み、これにより、データの複製を困難にしていた。

【０００３】

【発明が解決しようとする課題】しかし、従来の集積回路に接続された回路とデータの入出力を行う集積回路においては、複製防止データを組み込んだデータを用いる場合であっても、集積回路が実動作しているとき、集積回路に入出力するデータをサンプルすることにより、データの部分的な複製が可能であり、これを防止することはできないという問題があった。

【０００４】本発明は、このような問題を解消し、プログラムまたはデータの複製防止機能を有する集積回路を提供することを目的とする。

【０００５】

2

【課題を解決するための手段】本発明の集積回路は、上記課題を解決するために、集積回路の機能に基づく種々の動作を行う主回路手段と、入出力されるデータを暗号化または解読する暗号処理手段とを有する。

【０００６】

【作用】本発明によれば、入出力されるデータを暗号化または解読する暗号処理手段を具備しているから、主回路手段から出力されるデータを暗号化して外部装置へ出力するか、または外部装置から入力される暗号化されたデータを解読して主回路手段へ出力することができる。そして、集積回路と外部装置との間で入出力されるデータは暗号化されたデータであるから、入出力されるデータを複製しても、解読手段がなければこのデータを利用することができない。したがって、主回路の機能のみを複製した回路ではこのデータを使用することができない。また、データが暗号化されているため、主回路の複製も困難である。

【０００７】

【実施例】次に図面を用いて本発明の実施例を説明する。図１に、本発明による集積回路の一実施例を示す。図１は、集積回路と外部回路とが接続された状態を示す。集積回路１は主回路１１および暗号化・解読回路１２を備えている。主回路１１は、集積回路１の主な機能を実現するものであり、集積回路１の機能に基づく種々の動作を行う。主回路１１は、たとえばＣＰＵによって構成される。

【０００８】暗号化・解読回路１２は、データの暗号化および暗号化されたデータの解読の機能を有する回路であり、同図に示すように暗号化回路１２ａと解読回路１２ｂとにより構成されている。暗号化回路１２ａは主回路１１から入力されるデータを暗号化して外部回路２へ出力し、解読回路１２ｂは外部回路２から入力されるデータを解読して主回路１１へ出力する。

【０００９】暗号化の方式としては種々のものを用いることが可能であるが、本実施例においてはＵＳＡスタンダード暗号化方式（ＤＥＳ）をベースとしたアルゴリズムにより暗号化を行う。

【００１０】ＤＥＳは、０と１からなる２元データに対するブロック暗号であり、２元データを６４ビットのブロックに分割し、各ブロックについて転置と換字を繰り返すことにより暗号化を行うものである。この場合に転置はあらかじめ固定された変換であるが、換字には６４ビットのキーが使用され、このキーによって換字が制御される。一方、復号すなわち解読においては、暗号化とは逆に換字および転置が繰り返される。

【００１１】暗号化・解読回路１２には外部回路２が接続されている。外部回路２は集積回路１との間でデータを授受する外部装置であり、たとえば集積回路１から出力されるデータを記憶する記憶装置、または集積回路１によって処理されるデータを読み出す記憶装置である。

なお、図示しないが、データの入出力を制御するインタフェース制御回路たる入出力回路を暗号化・解読回路１２に接続し、この入出力回路を通して外部回路２とのデータの授受を行うようにしてもよい。

【００１２】この装置によれば、集積回路１が外部回路２にデータを出力する場合、主回路１１により処理され出力されたデータは暗号化・解読回路１２に入力され、暗号化回路１２ａにより暗号化される。暗号化回路１２ａに入力されたデータは前述のような暗号化によって暗号化されたデータに変換される。暗号化されたデータは、外部回路２へ出力される。

【００１３】一方、外部回路２から集積回路１へデータが入力される場合には、外部回路２から入力される暗号化されたデータは暗号化・解読回路１２の解読回路１２ｂで解読された後、主回路１１に供給され所定の処理が行われる。

【００１４】このように暗号化・解読回路１２により暗号化されたデータが外部装置２へ出力され、また、外部装置２からは暗号化されたデータが入力された暗号化・解読回路１２により解読される。したがって、外部装置２との間で入出力されるデータは暗号化されたデータであるから、集積回路１に入出力されるデータを複製しても解読手段を持たない限り、複製したデータを利用することができず、主回路１１の機能のみを複製した回路ではこのデータを使用することができない。また、データが暗号化されているため、主回路１１の複製も困難である。

【００１５】図２には、外部回路２として記憶装置２１を接続した場合の例が示されている。記憶装置２１は、集積回路１によって処理され、出力されたデータを記憶する記憶装置であり、集積回路１から出力される暗号化されたデータが格納される。この場合には、図１の暗号化・解読回路１２の機能は暗号化機能のみで十分であるから、暗号化回路１２ａに置き換えられている。

【００１６】このように接続された装置において、第三者が記憶装置２１に格納されたデータを複製した場合にも、複製データを得た者はこのデータを解読する手段を持たない限り、このデータを利用することができない。したがって、集積回路１は複製から保護される。

【００１７】図３には、外部回路２として読み出し専用の記憶装置２２が使用された場合の例が示されている。この場合には記憶装置２２にあらかじめ格納された暗号化されたデータが集積回路１へ読み出され、処理される。この場合には、図１の暗号化・解読回路１２の機能は解読機能のみで十分であるから、解読回路１２ｂに置き換えられている。記憶装置２２に格納されるデータは主回路１１が必要とするデータをあらかじめ暗号化したデータである。この暗号化はたとえば前述のＤＥＳによって行われる。図６に示すように、主回路１１が必要とする主回路データを供給し（ステップ３１）、このデータをブロックに分割し（ステップ３２）、転置および換字を所定の回数繰り返して暗号化を行い（ステップ３３）、暗号化されたデータを得て記憶装置２２に格納する（ステップ３４）。

【００１８】図４には、本発明による集積回路が２個接続された場合の例が示されている。集積回路４１は、主回路４１１および暗号化・解読回路４１２を有し、暗号化・解読回路４１２は暗号化回路４１２ａおよび解読回路４１２ｂを含んでいる。同様に、集積回路４２は主回路４２１および暗号化・解読回路４２２を有し、暗号化・解読回路４２２は暗号化回路４２２ａおよび解読回路４２２ｂを含んでいる。暗号化回路４１２ａは解読回路４２２ｂに接続され、暗号化回路４２２ａは解読回路４１２ｂに接続されている。

【００１９】この装置によれば、集積回路４１の主回路４１１から出力されたデータは暗号化回路４１２ａで暗号化され、集積回路４２の解読回路４２２ｂで解読された後、主回路４２１へ送られる。また、集積回路４２の主回路４２１から出力されたデータは暗号化回路４２２ａで暗号化され、集積回路４１の解読回路４１２ｂで解読された後、主回路４１１へ送られる。

【００２０】集積回路４１の主回路４１１と集積回路４２の主回路４２１の主回路としての機能は通常異なるものである。また、集積回路４１の行う暗号化と集積回路４２の行う暗号化のアルゴリズムは同じものである必要はないが、暗号化回路４１２ａが生成する暗号を解読回路４２２ｂが解読でき、かつ、暗号化回路４２２ａが生成する暗号を解読回路４１２ｂが解読できるようにされている。集積回路４１と集積回路４２の暗号化アルゴリズムが異なる場合には、データ複製防止機能はさらに向上する。

【００２１】図５には、本発明による集積回路がワンチップマイクロコンピュータ６および入出力用集積回路６３として用いられ、これらが互いに接続されるとともに、メモリ６４に接続された場合の一例が示されている。ワンチップマイクロコンピュータ６はＣＰＵ６１、暗号化・解読回路６２ａおよび暗号化・解読回路６２ｂを有しており、ＣＰＵ６１が図１の主回路１１に相当する。入出力用集積回路６３は、暗号化・解読回路６３１および入出力回路６３２を有し、入出力回路６３２が図１の主回路１１に相当する。

【００２２】ワンチップマイクロコンピュータ６の暗号化・解読回路６２ａは、入出力用集積回路６３の暗号化・解読回路６３１と接続され、暗号化・解読回路６２ｂはメモリ６４と接続されている。入出力用集積回路６３の入出力回路６３２は入出力端子６５を介して外部装置と接続されている。

【００２３】ワンチップマイクロコンピュータ６に接続されたメモリ６４には、ＣＰＵ６１のプログラムとデータが暗号化されたデータとして格納されている。メモリ

６４から読み出されたプログラムおよびデータは暗号化・解読回路６２ｂにおいて解読され、ＣＰＵ６１に送られる。ＣＰＵ６１はこのプログラムおよびデータにより所定の処理を行う。

【００２４】また、ＣＰＵ６１からのデータは暗号化・解読回路６２ａにおいて暗号化されて入出力用集積回路６３の暗号化・解読回路６３１に送られ、暗号化・解読回路６３１で解読された後、入出力回路６３２に送られる。そして入出力回路６３２で入出力処理を行われた後、入出力端子６５を通して外部装置へ出力される。逆に、外部装置から入出力端子６５を通して入力されたデータは、入出力回路６３２で入出力処理を行われた後、暗号化・解読回路６３１に送られて暗号化され、ワンチップマイクロコンピュータ６の暗号化・解読回路６２ａへ出力される。データは暗号化・解読回路６２ａで解読され、ＣＰＵ６１に送られる。ＣＰＵ６１で処理されたデータは暗号化・解読回路６２ｂにおいて暗号化され、メモリ６４に記憶される。

【００２５】本装置においても、前述のような暗号化アルゴリズムによって暗号化されたデータがワンチップマイクロコンピュータ６、入出力用集積回路６３およびメモリ６４の間で入出力される。

【００２６】一般に乱数を用いた暗号化や暗号化鍵によるビット反転とビット入れ換え操作を多段数行う暗号化では、暗号化アルゴリズムを知らずに暗号化されたデータやプログラムを解読することは、非常に困難である。また、集積回路のマスクパターンから暗号化アルゴリズムを解析するか、あるいは、ＣＰＵ６１と暗号化・解読回路６２ａ，６２ｂの間の信号を解析することが非常に困難であることは言うまでもない。

【００２７】図５の実施例においては、メモリ６４に格納されたデータまたはプログラムを複製しても、このデータを解読しないかぎり利用できないため、ＣＰＵ６１のデータまたはプログラムを保護することができる。また、入出力用集積回路６３に対するコマンドやデータが暗号化されていることにより、入出力集積回路６３のコマンド体系やデータ形式が保護されるため、入出力集積回路６３の複製を防止できる。

【００２８】

【発明の効果】以上説明したように本発明によれば、集

積回路には暗号化されたデータが入出力されるから、入出力されるデータを複製しても、主回路の機能のみを複製した回路ではこのデータを使用することができない。暗号化されたデータを解読するには暗号化アルゴリズムを調査しデータを解読するか、または、集積回路の内部で主回路と暗号化・解読回路の間の信号を直接サンプリングしなければならないため、データの複製は非常に困難である。また、データを暗号化しているため主回路の複製も困難であるから、回路を複製から有効に保護することができる。

【図面の簡単な説明】

【図１】本発明による集積回路の一実施例を示すブロック図である。

【図２】本発明による集積回路を記憶装置に接続した実施例を示すブロック図である。

【図３】本発明による集積回路を読み出し専用記憶装置に接続した実施例を示すブロック図である。

【図４】本発明による集積回路を２個接続した実施例を示すブロック図である。

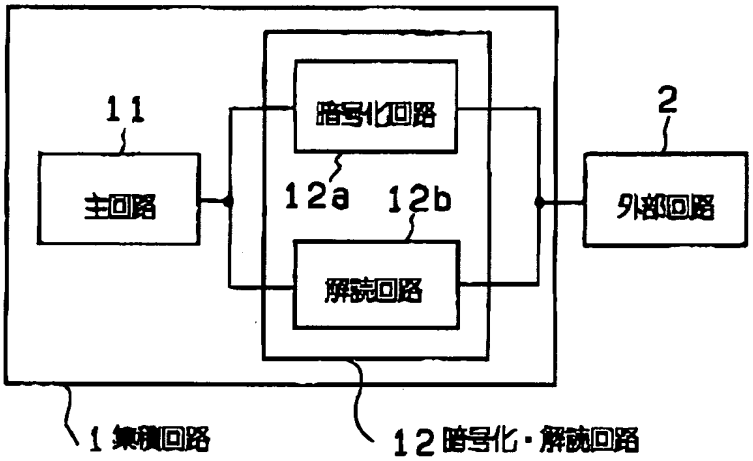
【図５】本発明による集積回路をワンチップマイクロコンピュータおよび入出力用集積回路として用いた実施例を示すブロック図である。

【図６】暗号化データを作成する手順を示すフロー図である。

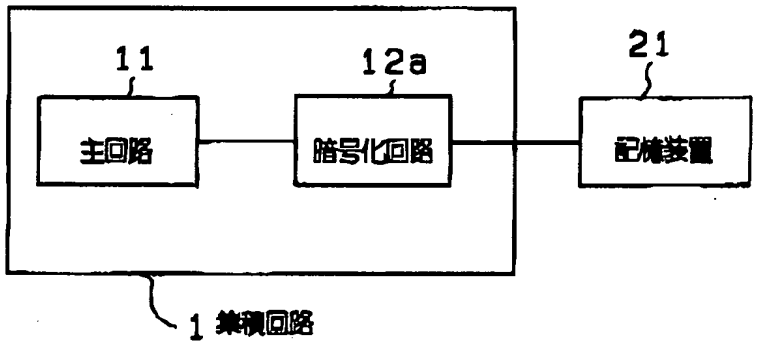
【符号の説明】

１　集積回路
２　外部回路
６　ワンチップマイクロコンピュータ
１２　暗号化・解読回路
２１　記憶装置
２２　記憶装置
４１　集積回路
４２　集積回路
６１　ＣＰＵ
６２ａ　暗号化・解読回路
６２ｂ　暗号化・解読回路
６３　入出力集積回路
６４　メモリ
６５　入出力端子

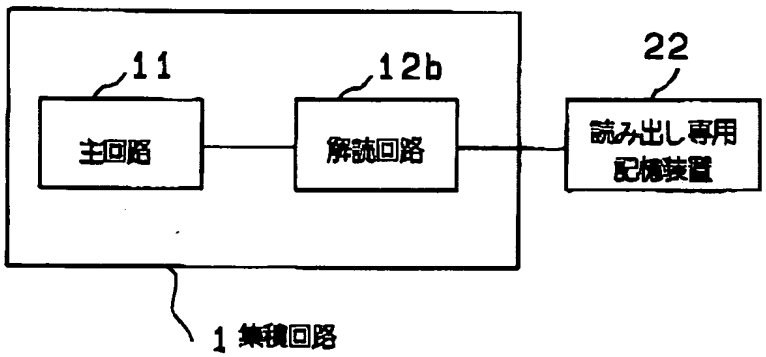
【図1】


11
暗号化回路
2
主回路
12a
12b
外部回路
解読回路
1 集積回路
12 暗号化・解読回路

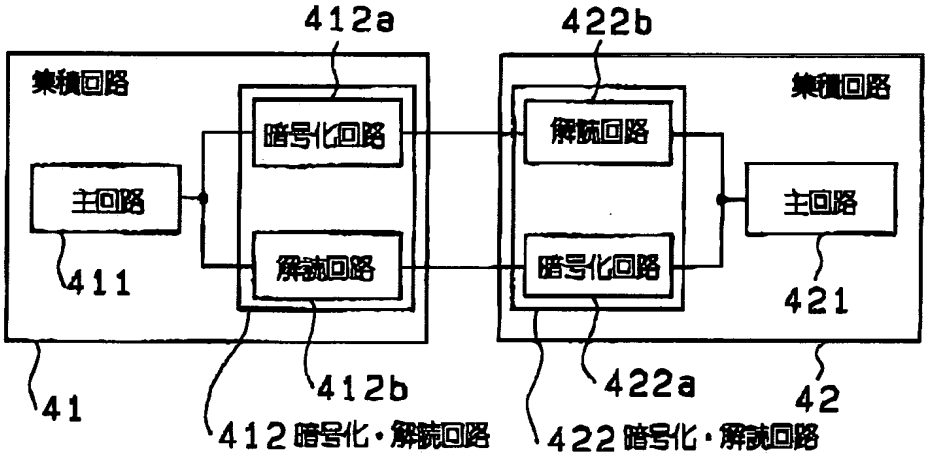
【図2】


11
12a
21
主回路
暗号化回路
記憶装置
1 集積回路

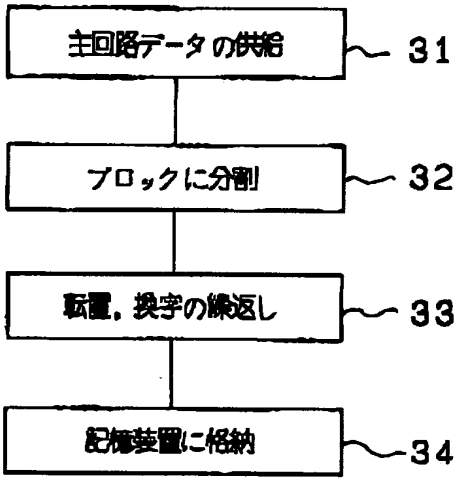
【図3】


11
12b
22
主回路
解読回路
読み出し専用
記憶装置
1 集積回路

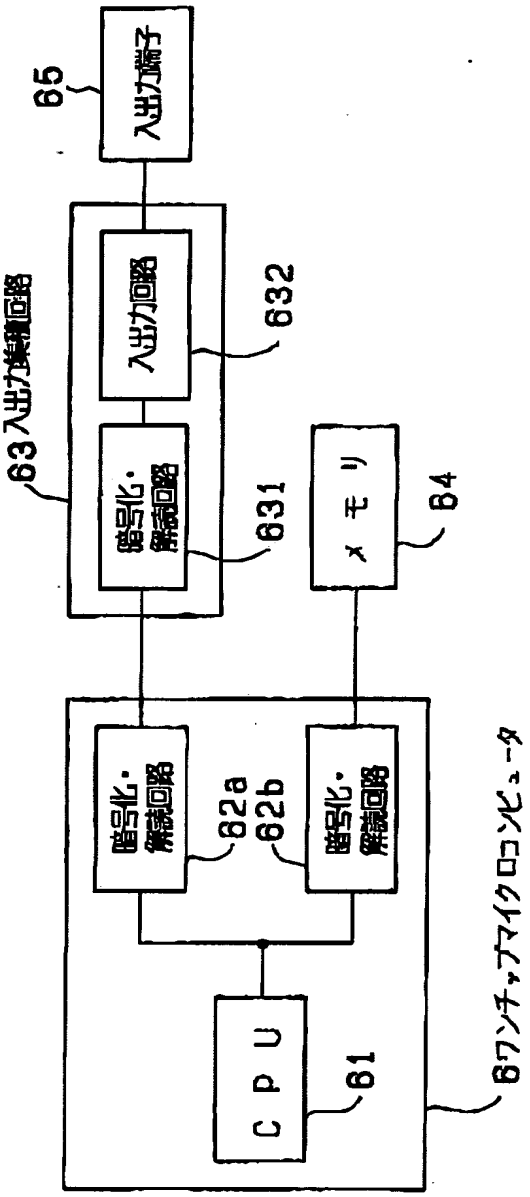
【図4】


412a
422b
集積回路
暗号化回路
解読回路
主回路
411
解読回路
暗号化回路
主回路
421
集積回路
41
412b
422a
42
412 暗号化・解読回路
422 暗号化・解読回路

【図6】


主回路データの供給
31
ブロックに分割
32
転置，換字の繰返し
33
記憶装置に格納
34

【図5】


65
入出力端子
63入出力制御回路
入出力回路
632
暗号化・解読回路
631
メモリ
64
暗号化・解読回路
82a
62b
暗号化・解読回路
CPU
61
6ワンチップマイクロコンピュータ